Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method for providing content identification within a media data stream for distribution from a media content data source device comprising:

receiving the data stream of media content at the media content data source device; and

inserting content identification data into frames of the media data stream, in conjunction with each data frame for which a corresponding content identification data relates, at regular intervals within the media data stream to be distributed, wherein the content identification data includes a tamper resistant identifier that (a)(i) is based upon a rapidly changing property extracted from a given data frame of the media data stream that is difficult to alter and (a)(ii) is inserted into the media data stream in conjunction with the corresponding given data frame by reference to the rapidly changing property from which property data was extracted, further wherein the rapidly changing property of the media data stream includes a property which changes with each frame of the media data stream, the content identification data further comprising a continuity count within the identifier, wherein the continuity count comprises a data field that increments in a predictable manner each time the identifier is inserted into the media data stream to enable a detection of unauthorized editing by detecting any discontinuity in an embedded continuity count, wherein inserting content identification data further comprises:

extracting data relating to a predetermined property of the media data stream;

combining the extracted data with content identification data by forming a hash code from (b)(i) the extracted data and (b)(ii) the content identification data;

applying a digital signature to the hash code of combined data that includes applying both (c)(i) a digital signature of the originator of the media data stream and (c)(ii) a digital signature of a corresponding certification authority; and

inserting the combined data and digital signature as secured content identification data into the data stream.

2. (Original) The method of claim 1 wherein the content identification data is inserted every frame.

3. (Original) The method of claim 1 wherein the content identification data is digitally combined with a predetermined property of the data stream.

4. (Canceled)

5. (Canceled)

6. (Original) The method of claim 1 in which the media data stream may comprise any one or more of pictures and audio or video data streams.

7. (Original) The method of claim 3 in which the predetermined property is any property of the media data stream that changes from data frame to data frame.

8. (Previously Presented) The method of claim 7 in which the predetermined property comprises any one or more of: frame size, frame hash, transport stream identifier, and clock signal.

9. (Original) The method of claim 8 in which the predetermined property is a combination of frame size and frame hash.

10. (Canceled)

11. (Currently Amended) A method of transcoding a media data stream for distribution from a transcoder device, the method comprising:

receiving a data stream of media content from a media content data source device, the data stream of media content including embedded, secured content identification data in frames of the media data stream, in conjunction with each data frame for which a corresponding content identification data relates, at regular intervals within the media data stream, in which the secured content identification data incorporates data relating to a predetermined property of the media data stream and that corresponds to a tamper resistant identifier that (a)(i) is based upon a rapidly changing property extracted from a given data frame of the media data stream that is difficult to alter and (a)(ii) is inserted into the media data stream in conjunction with the corresponding given data frame by reference to the rapidly changing property from which property data was extracted, further wherein the rapidly changing property of the media data stream includes a property which changes with each frame of the media data stream, the content identification data further including a continuity count within the identifier, wherein the continuity count comprises a data field that increments in a predictable manner each time the identifier is inserted into the media data stream to enable a detection of unauthorized editing by detecting any discontinuity in an embedded continuity count, wherein inserted content identification data further comprises extracted data relating to a predetermined property of the media data stream, the extracted data being combined with content identification data by forming a hash code from (b)(i) the extracted data and (b)(ii) the content identification data, a digital signature being applied to the hash code of combined data that includes applying both (c)(i) a digital signature of the originator of the media data stream and (c)(ii) a digital

signature of a corresponding certification authority, and the combined data and digital signature being embedded as the secured content identification data in the data stream;

transcoding the media content of the data stream into a new format;

extracting data relating to a predetermined property of the media data stream in its new format;

extracting content identification data from the secured content identification data;

combining the extracted data with the extracted content identification data by forming a hash code from (d)(i) the extracted data and (d)(ii) the content identification data;

applying a digital signature to the hash code of combined data that includes applying a digital signature of the transcoding device and making available a corresponding public key of the transcoding device that is digitally signed by the originator of the content identification data; and

inserting the combined data and digital signature as re-secured content identification data into the data stream corresponding to a transcoded data stream output by the transcoder device.

12. (Original) The method of claim 11 in which the new format of the data stream has a lower resolution or transmission / storage bandwidth than the original format of the data stream.

13. (Previously Presented) The method of claim 11 in which the media content may comprise any one or more of pictures, audio, and video data streams.

14. (Original) The method of claim 11 in which the predetermined property is any property of the media data stream that changes from data frame to data frame.

15. (Previously Presented) The method of claim 14 in which the predetermined property comprises any one or more of: frame size, frame hash, transport stream identifier, and clock signal.

16. (Original) The method of claim 15 in which the predetermined property is a combination of frame size and frame hash.

17. (Canceled)

18. (Canceled)

19. (Previously Presented) The method of claim 11 in which the combining the extracted data with the extracted content identification data further includes modifying the extracted content identification data.

20. (Previously Presented) The method of claim 19 in which the modifying the extracted content identification data comprises including an indication of the new format of the transcoded data stream.

21. (Previously Presented) The method of claim 19 in which the modifying the extracted content identification data comprises including an identity of the transcoder device performing the transcoding.

22. (Currently Amended) A method of verifying the integrity of secured content identification data embedded in a media data stream with a receiver device, comprising:

receiving a data stream of media content by the receiver device, the data stream of media content including embedded, secured content identification data in frames of the media data stream, in conjunction with each data frame for which a corresponding

content identification data relates, at regular intervals within the media data stream, in which the secured content identification data incorporates data relating to a predetermined property of the media data stream and that corresponds to a tamper resistant identifier that (a)(i) is based upon a rapidly changing property extracted from a given data frame of the media data stream that is difficult to alter and (a)(ii) is inserted into the media data stream in conjunction with the corresponding given data frame by reference to the rapidly changing property from which property data was extracted, further wherein the rapidly changing property of the media data stream includes a property which changes with each frame of the media data stream, the content identification data further including a continuity count within the identifier, wherein the continuity count comprises a data field that increments in a predictable manner each time the identifier is inserted into the media data stream to enable a detection of unauthorized editing by detecting any discontinuity in an embedded continuity count, wherein inserted content identification data further comprises extracted data relating to a predetermined property of the media data stream, the extracted data being combined with content identification data by forming a hash code from (b)(i) the extracted data and (b)(ii) the content identification data, a digital signature being applied to the hash code of combined data that includes applying both (c)(i) a digital signature of the originator of the media data stream and (c)(ii) a digital signature of a corresponding certification authority, and the combined data and digital signature being embedded as the secured content identification data in the data stream;

extracting first data relating to a predetermined property of the media data stream;

extracting content identification data from the secured content identification data;

extracting second data relating to the predetermined property from the secured content identification data; and

comparing the first data and the second data to verify the authenticity of the extracted content identification data.

23. (Previously Presented) The method of claim 22 in which the extracting content identification data from the secured content identification data comprises:

obtaining a public key of a content provider that secured the content identification data; and

verifying an encrypted signature of the content provider using the public key.

24. (Previously Presented) The method of claim 23 in which the extracting content identification data from the secured content identification data comprises:

obtaining a public key of a certification authority;

verifying the authenticity of the public key of the content provider using the public key of the certification authority.

25. (Previously Presented) The method of claim 22 in which the media data stream is received via a transcoding device, and in which the extracting content identification data from the secured content identification data comprises verifying that the transcoder device was authorised to modify the data stream by an originator of the content identification data.

26. (Previously Presented) The method of claim 25 in which the extracting content identification data from the secured content identification data comprises:

obtaining a public key of the transcoding device that secured the content identification data, the public key being digitally signed by the originator of the content identification data;

obtaining a public key of the originator;

verifying an encrypted signature of the originator using the public key of the originator, and thereby verifying the public key of the transcoder device;

verifying the content identification information using the verified public key of the transcoder device.

27. (Previously Presented) The method of claim 22 in which the media content data stream may comprise any one or more of pictures, audio, and video data streams.

28. (Original) The method of claim 22 in which the predetermined property is any property of the media data stream that changes from data frame to data frame.

29. (Previously Presented) The method of claim 28 in which the predetermined property comprises any one or more of: frame size, frame hash, transport stream identifier, and clock signal.

30. (Original) The method of claim 29 in which the predetermined property is a combination of frame size and frame hash.

31. (Currently Amended) Apparatus for providing content identification within a media data stream to be distributed, comprising:

means for receiving a data stream of media content;

means for inserting content identification data into frames of the media data stream, in conjunction with each data frame for which a corresponding content identification data relates, at regular intervals within the media data stream to be distributed, wherein the content identification data includes a tamper resistant identifier that (a)(i) is based upon a rapidly changing property extracted from a given data frame of the media data stream that is difficult to alter and (a)(ii) is inserted into the media data stream in conjunction with the corresponding given data frame by reference to the rapidly changing property from which property data was extracted, further wherein the rapidly changing property of the media data stream includes a property which changes

with each frame of the media data stream, the content identification data further comprising a continuity count within the identifier, wherein the continuity count comprises a data field that increments in a predictable manner each time the identifier is inserted into the media data stream to enable a detection of unauthorized editing by detecting any discontinuity in an embedded continuity count, wherein inserted content identification data further comprises extracted data relating to a predetermined property of the media data stream, the extracted data being combined with content identification data by forming a hash code from (b)(i) the extracted data and (b)(ii) the content identification data, a digital signature being applied to the hash code of combined data that includes applying both (c)(i) a digital signature of the originator of the media data stream and (c)(ii) a digital signature of a corresponding certification authority, and the combined data and digital signature being embedded as the secured content identification data in the data stream.

32. (Currently Amended) The apparatus of claim 31 wherein the means for inserting comprises:

a data extraction module for extracting data relating to [[a]] the predetermined property of the media data stream;

means for combining the extracted data with content identification data;

an encryption module for applying [[a]] the digital signature to the combined data; and

a data merge module for inserting the combined data and digital signature as secured content identification data into the data stream.

33. (Currently Amended) The apparatus of claim 32 in which the means for combining includes a hash function generator for forming [[a]] the hash code from the combined data, the encryption module applying the digital signature to the hash code.

34. (Currently Amended) Apparatus for transcoding a media data stream to be distributed, comprising:

means for receiving a data stream of media content from a media content data source device, the data stream of media content including embedded, secured content identification data in frames of the media data stream, in conjunction with each data frame for which a corresponding content identification data relates, at regular intervals within the media data stream, in which the secured content identification data incorporates data relating to a predetermined property of the media data stream and that corresponds to a tamper resistant identifier that (a)(i) is based upon a rapidly changing property extracted from a given data frame of the media data stream that is difficult to alter and (a)(ii) is inserted into the media data stream in conjunction with the corresponding given data frame by reference to the rapidly changing property from which property data was extracted, further wherein the rapidly changing property of the media data stream includes a property which changes with each frame of the media data stream, the content identification data further including a continuity count within the identifier, wherein the continuity count comprises a data field that increments in a predictable manner each time the identifier is inserted into the media data stream to enable a detection of unauthorized editing by detecting any discontinuity in an embedded continuity count, wherein inserted content identification data further comprises extracted data relating to a predetermined property of the media data stream, the extracted data being combined with content identification data by forming a hash code from (b)(i) the extracted data and (b)(ii) the content identification data, a digital signature being applied to the hash code of combined data that includes applying both (c)(i) a digital signature of the originator of the media data stream and (c)(ii) a digital signature of a corresponding certification authority, and the combined data and digital signature being embedded as the secured content identification data in the data stream;

a transcoder module for transcoding the media content of the data stream into a new format;

a data extraction module for extracting data relating to a predetermined property of the media data stream in its new format and for extracting content identification data from the secured content identification data;

means for combining the extracted data with the extracted content identification data;

an encryption module for applying a digital signature to the combined data; and

a data merge module for inserting the combined data and digital signature as re-secured content identification data into the data stream corresponding to a transcoded data stream to be output by the transcoding apparatus.

35. (Currently Amended) Apparatus for verifying the integrity of secured content identification data embedded in a media data stream, comprising:

means for receiving a data stream of media content including embedded, secured content identification data in frames of the media data stream, in conjunction with each data frame for which a corresponding content identification data relates, at regular intervals within the media data stream, in which the secured content identification data incorporates data relating to a predetermined property of the media data stream and that corresponds to a tamper resistant identifier that (a)(i) is based upon a rapidly changing property extracted from a given data frame of the media data stream that is difficult to alter and (a)(ii) is inserted into the media data stream in conjunction with the corresponding given data frame by reference to the rapidly changing property from which property data was extracted, further wherein the rapidly changing property of the media data stream includes a property which changes with each frame of the media data stream, the content identification data further including a continuity count within the identifier, wherein the continuity count comprises a data field that increments in a predictable manner each time the identifier is inserted into the media data stream to enable a detection of unauthorized editing by detecting any discontinuity in an embedded continuity count, wherein inserted content identification

data further comprises extracted data relating to a predetermined property of the media data stream, the extracted data being combined with content identification data by forming a hash code from (b)(i) the extracted data and (b)(ii) the content identification data, a digital signature being applied to the hash code of combined data that includes applying both (c)(i) a digital signature of the originator of the media data stream and (c)(ii) a digital signature of a corresponding certification authority, and the combined data and digital signature being embedded as the secured content identification data in the data stream;

a data extraction module for extracting first data relating to a predetermined property of the media data stream;

a decryption module for extracting content identification data from the secured content identification data; and for extracting second data relating to the predetermined property from the secured content identification data; and

a compare module for comparing the first data and the second data to verify the authenticity of the extracted content identification data.

36. (Previously Presented) A computer program product, comprising a computer-executable program code stored on a computer readable medium having thereon computer program code means adapted, when said program code is loaded onto a computer, to make the computer execute the procedure of claim 1.

37. (Canceled).